|  |
| --- |
| Vejledning |
| **Vejledning og eksempel på politik om personoplysninger i ansættelsesforholdet mv.** |
| December 2021 |

**Baggrund**

En virksomhed håndterer løbende en række oplysninger om medarbejderne. Det gælder både ved ansættelse, i det løbende ansættelsesforhold, og når et ansættelsesforhold ophører.

I den forbindelse har virksomheden som dataansvarlig en række pligter overfor medarbejderne.

Virksomheden må kun registrere oplysninger om medarbejderne, hvis der er en lovlig grund til det. Fx hvis det er nødvendigt for at opfylde ansættelseskontrakten. Du kan læse mere om de lovlige grunde (”hjemmelsgrundlaget”) i Dansk Erhvervs Vejledning om virksomhedens håndtering af medarbejderoplysninger. Du finder vejledningen på [www.danskerhverv.dk](http://www.danskerhverv.dk).

Medarbejderne har en række rettigheder, når virksomheden behandler oplysninger om dem. Virksomheden har som udgangspunkt pligt til at informere medarbejderne om en række forhold, og medarbejderne har i vidt omfang ret til indsigt, berigtigelse, sletning, indsigelse, begrænsning mv. af de registrerede oplysninger.

Dansk Erhverv har udarbejdet et eksempel på en persondatapolitik, der beskriver, hvordan virksomheden administrerer persondata om medarbejdere. Politikken er rettet mod alle medarbejdere i virksomheden og kan stå alene eller være en del af en personalehåndbog. Politikken skal naturligvis tilpasses de aktuelle forhold på virksomheden, og det kan være nødvendigt at omtale en række yderligere forhold, fx tv-overvågning, GPS, optagelser, logning af internetbrug og adgang til e-mails fx via henvisning til selvstændige politikker. Politikken er vedlagt som **bilag 1**,

Dansk Erhverv har derudover blandt andet udarbejdet eksempler på politikker og vejledninger om

* IT-sikkerhed
* Tv-overvågning
* GPS-sporing

Du kan finde politikkerne og vejledningerne på [www.danskerhverv.dk](http://www.danskerhverv.dk).

I politikken er en henvisning til ”Sikkerhedspolitik ved personaleadministration". Dansk Erhverv har udarbejdet et eksempel på en sådan politik, der kan hentes på [www.danskerhverv.dk](http://www.danskerhverv.dk).

Datatilsynet har udgivet en vejledning om databeskyttelse i forbindelse med ansættelsesret.

Nedenfor vil vi særligt knytte et par bemærkninger til sletning af oplysninger og overførsel af persondata til tredjelande.

*Sletning*

Hvis det er muligt, skal du oplyse de forventede tidsfrister for sletning. Slettefristerne skal angives for de forskellige kategorier af oplysninger, som virksomheden behandler i forbindelse med personaleadministrationen.

Databeskyttelsesreglerne indeholder et generelt krav om, at en virksomhed ikke må opbevare oplysninger på en måde, der giver mulighed for at identificere den registrerede i længere tid end det, der er nødvendigt til behandlingsformålet. En virksomhed skal derfor løbende overveje, om det er nødvendigt at opbevare en oplysning – og ellers slette den. Har din virksomhed fastsat generelle slettefrister, følger det dog af Datatilsynets nuværende praksis, at virksomheden ikke har pligt til løbende at gennemgå samtlige sager, dokumenter mv. med henblik på at sikre, at der ikke behandles oplysninger i strid hermed. Det forudsætter dog, at virksomheden har procedurer som sikrer, at det sker sletning i overensstemmelse med de fastsatte frister.[[1]](#footnote-2)[1]

Det er Dansk Erhvervs vurdering, at en virksomhed som udgangspunkt må have mulighed for at opbevare en personalesag 5 år efter medarbejderens fratræden som følge af den almindelige 5-årige forældelsesfrist i ansættelsesretlige sager. Virksomheden skal også overholde bogføringslovens regler herunder opbevaring af relevante oplysninger i denne sammenhæng i 5 år efter et regnskabsårs afslutning. Samtidig kan der være situationer, hvor særlige forhold gør en længere opbevaringsperiode relevant, f.eks. verserende arbejdsskadesager, uafsluttede retssager eller arbejdsretlige tvister mellem medarbejderen og virksomhed, pensionsforpligtelser, dagpengerefusion og udbetaling af tilgodehavender.

*Overførsel til tredjelande*

Ønsker I at overføre personoplysninger til et tredjeland (eller en international organisation), skal databeskyttelsesforordningens særlige regler om sådanne overførsler overholdes. I kan læse mere om kravene til sådanne overførsler i Datatilsynets ”Vejledning om overførsel af personoplysninger til tredjelande fra juli 2021”.

**Medarbejderens egen håndtering af persondata**

Virksomheden skal også overholde databeskyttelsesreglerne, når medarbejderne håndterer persondata om fx kunder. Her er medarbejderne forpligtede til at overholde de retningslinjer for behandling af persondata, som virksomheden udstikker. Samtidig er det vigtigt, at medarbejderne orienterer virksomheden, hvis der sker sikkerhedsbrud.

Dansk Erhverv har udarbejdet en kort instruks fra virksomheden til medarbejderen vedrørende medarbejdernes egen behandling af personoplysninger, samt om hvordan medarbejderen skal forholde sig ved sikkerhedsbrud. Teksten er vedlagt som **bilag 2**.

**Bilag 1. Eksempel på politik om personoplysninger i ansættelsesforholdet**

**Håndtering af personoplysninger om ansatte hos [virksomhedens navn]**

[Virksomhedens navn] håndterer løbende en række forskellige personoplysninger om vores medarbejdere. [Virksomhedens navn, cvr.nr., kontaktinfo] er dataansvarlig i forhold til behandlingen af oplysninger om dig.

**Ansættelse i [Virksomhedens navn]**

Når du bliver ansat hos os, opretter vi en personalesag med dine oplysninger [fysisk og/eller i hvilket system]. I personalesagen registrerer og opbevarer vi de oplysninger, der er nødvendige og relevante i forhold til din ansættelse hos os. Dermed indsamler og opbevarer vi en række personoplysninger om dig.

Fx indsamler og opbevarer vi de oplysninger, som vi har modtaget i forbindelse med ansættelsen, herunder bl.a. ansøgning, CV, referencer, eksamensbeviser, mv.

Vi indsamler og opbevarer også de oplysninger, der løbende måtte være nødvendige og relevante i forbindelse med håndteringen af dit ansættelsesforhold. De indsamlede oplysninger kan dels kategoriseres som *almindelige personoplysninger*, jf. databeskyttelsesforordningens art. 6 og dels som *følsomme oplysninger*, jf. databeskyttelsesforordningens art. 9.

Vi indsamler og opbevarer således følgende oplysninger med det formål at kunne foretage personaleadministration: [*Indskriv andet formål/legitim interesse, hvis formålet/legitime interesse ikke er ”personaleadministration* ”].

Som udgangspunkt sker behandlingen af dine oplysninger med henblik på opfyldelse af din ansættelseskontrakt og det løbende ansættelsesforhold, jf. § 6, stk. 1, litra b i databeskyttelsesforordningen. Hvor der er andre mulige behandlingsgrundlag, er disse angivet nedenfor under de enkelte oplysninger.

[*skal tilpasses de aktuelle forhold på virksomheden]*:

|  |
| --- |
| Kontakt- og identifikationsoplysninger |
| Navn, privat adresse, e-mail og telefonnummer |
| Hjemmeside og intranet  *På intranettet registrerer vi følgende oplysninger om dig: Navn, stilling, afdeling, direkte telefonnummer og e-mail. Herudover lægger vi et billede af dig på intranettet. Alt sammen for at dine kolleger lettere kan finde dig. (Forfølgelse af legitim interesse, jf. persondataforordningens art. 6, stk. 1, litra f)*  *På vores hjemmeside registrerer vi følgende oplysninger om dig: Navn, stilling, direkte telefonnummer og e-mail. Herudover lægger vi et billede af dig på hjemmesiden, hvis du har givet samtykke hertil.*  *Billedet behandles (Samtykke, jf. persondataforordningens art. 6, stk. 1, litra a og forfølgelse af en legitim interesse, jf. persondataforordningens art. 6, stk. 1, litra f).* |
| CPR-nr.  *(Nødvendig for at overholde en retlig forpligtigelse, jf. persondataforordningens art. 6, stk. 1, litra c samt databeskyttelseslovens § 11, stk. 2).* |
| Kontaktoplysninger på dine nærmeste pårørende  *(Den registreredes vitale interesse, jf. persondataforordningens art. 6, stk. 1, litra d)* |
| Arbejdsrelevante oplysninger |
| Arbejdssted, arbejdsopgaver, stillingsbetegnelse, arbejdstid, herunder vagt- og tjenestetider |
| Oplysninger om ansættelsesform, herunder fleksjob eller ansættelse på særlige vilkår |
| Skatte- og bankoplysninger |
| Fraværsoplysninger |
| Ferie og andet fravær  *(Nødvendig for at overholde en retlig forpligtigelse, jf. persondataforordningens art. 6, stk. 1, litra c).* |
| Sygefravær  *(Nødvendig for at overholde en retlig forpligtigelse, jf. persondataforordningens art. 6, stk. 1, litra c).* |
| Orlov, herunder graviditets, barsels, fædre/medmor-orlov  *(Nødvendig for at overholde en retlig forpligtigelse, jf. persondataforordningens art. 6, stk. 1, litra c).* |
| Personaleadministrative oplysninger |
| Uddannelse og kvalifikationer, tidligere ansættelsesforhold, kurser, kompetenceprofil, jobønsker, medarbejderudviklingssamtaler, bedømmelser, beskæftigelse, tillidshverv, lån af diverse effekter, eventuelle advarsler og lignende, m.v.  *(Forfølgelse af legitim interesse, jf. persondataforordningens art. 6, stk. 1, litra f).* |
| Referencer  (Samtykke, jf. persondataforordningens art. 6, stk. 1, litra a og databeskyttelseslovens § 12, stk. 3,).  Oplysninger indhentet på sociale medier, fx LinkedIn, Facebook, mv.  *(Forfølgelse af legitim interesse, jf. persondataforordningens art. 6, stk. 1, litra f, samt art. 9, stk. 2, litra e, hvis personen selv har offentliggjort følsomme oplysninger.)* |
| Arbejdsskader  *(Nødvendig for at overholde en retlig forpligtelse, jf. persondataforordningens art 6, stk. 1, litra c* ***og/eller*** *nødvendig for at et retskrav kan fastlægges, gøres gældende eller forsvares, jf. persondataforordningens art 9, stk. 2, litra f* ***og/eller*** *overholdelse af virksomhedens arbejdsretlige forpligtelser, jf. persondataforordningens art 9, stk. 2, litra b* ***og/eller*** *overholdelse af arbejdsmiljølovgivningen)* |
| Helbredsoplysninger  *(Nødvendig for at overholde en retlig forpligtigelse, jf. persondataforordningens art. 6, stk. 1, litra c* ***og*** *nødvendig for at retskrav kan fastlægges, gøres gældende eller forsvares, jf. persondataforordningens art 9, stk. 2, litra f* ***og/eller*** *Helbredsoplysningsloven* ***og/eller*** *Arbejdsmiljølovens kapitel 11).* |
| Personlighedstest  *(Forfølgelse af legitim interesse, jf. persondataforordningens art. 6, stk. 1, litra f* ***og*** *samtykke, jf. persondataforordningens art. 9, stk. 2, litra a, jf. art 6, stk. 1, litra a, hvis testen indeholder følsomme oplysninger).* |
| Fagforeningsmæssige tilhørsforhold [Angiv lovligt formål, fx til brug for kontingenttræk]  *(Nødvendig for at overholde arbejdsretlige forpligtelser, jf. databeskyttelseslovens § 12, stk. 1).* |
| Straffeattest, børneattest og oplysninger vedrørende sikkerhedsgodkendelser  (Databeskyttelseslovens § 8, stk. 3 [samt børneattestloven])  For så vidt angår sikkerhedsgodkendelse skal der henvises til relevant lovkrav herom. |
| Biometrisk data med henblik på identifikation  *(Samtykke, jf. persondataforordningens art. 9, stk. 2, litra a, jf. art. 6, stk. 1, litra a).* |
| Lønoplysninger |
| Fradrag i lønnen (fx betaling for kantineordning eller medarbejdergoder i øvrigt) |

Hvis der sker ændringer i dine oplysninger, registrerer vi ændringerne.

Der kan være særlige situationer, hvor vi håndterer oplysninger, der ikke fremgår af listen ovenfor, eller hvor oplysninger behandles på et andet grundlag. For eksempel oplysninger vi modtager i forbindelse med idømt straf, eller hvis begivenheder udløser et behov for, at andre oplysninger skal indsamles.

**Hvem har adgang til [Virksomhedens] personaleoplysninger?**

Din personalesag findes i [en fysisk mappe placeret [indsæt] / i virksomhedens [indsæt it-system]]. Sagen er adskilt fra andre personalesager.

Det er udelukkende følgende medarbejdere, der har adgang til din personalemappe: [angiv så få medarbejdere som muligt f.eks. specifikke medarbejdere eller ”medarbejdere i virksomhedens HR og økonomiafdeling, nærmeste chef og virksomhedens øverste ledelse].

**I øvrigt** [Hvis sådanne findes på virksomheden]

Vi henviser i øvrigt til følgende politikker:

* Politik om IT, e-mail, internet samt mobiltelefon
* Politik om TV-overvågning
* [andre politikker]

**Er dine oplysninger korrekte?**

Hvis oplysningerne om dig ændrer sig, skal du informere [virksomheden/HR/…] om dette, så vi kan registrere ændringerne.

**Dine rettigheder**

Du har efter databeskyttelsesreglerne en række rettigheder i forhold til vores behandling af oplysninger om dig.

*Ret til at se oplysninger (indsigt)*: Du kan bede om at få indsigt i de personoplysninger, som vi har registreret om dig efter reglerne om indsigtsret.

*Ret til berigtigelse*: Du har ret til at få berigtiget urigtige oplysninger om dig selv.

*Ret til sletning:* Se afsnittet nedenfor om ”Sletning”. I særlige tilfælde kan du have ret til at få slettet oplysninger om dig, før vores generelle slettefrister indtræffer.

*Ret til begrænsning af behandling*: Du kan i visse tilfælde have ret til at få behandlingen af dine personoplysninger begrænset.

*Ret til indsigelse:* Du kan i visse tilfælde have ret til at gøre indsigelse mod vores eller databehandleres behandling af dine personoplysninger.

*Ret til at trække samtykke tilbage*: Hvis du har givet samtykke til behandling af en eller flere personoplysninger om dig, kan du på ethvert tidspunkt trække dit samtykke tilbage efter de persondataretlige regler. Medmindre virksomheden har et andet lovligt behandlingsgrundlag, kan vi ikke længere behandle de pågældende oplysninger.

*Ret til at klage til Datatilsynet:* Du har ret til at klage til Datatilsynet over vores behandling af dine personoplysninger, hvis du mener, at behandlingen ikke sker efter gældende regler. Du kan finde Datatilsynets kontaktoplysninger på www.datatilsynet.dk.

**Videregivelse af personoplysninger**

I en række tilfælde skal eller kan [Virksomhedens navn] videregive dine relevante oplysninger til relevante modtagere, f.eks. [skal tilpasses de aktuelle forhold i virksomheden]

* SKAT vedr. skattepligtige ydelser
* Arbejdsmarkedets Tillægspension (ATP)
* ACF (Arbejdsgivernes Centrale Ferieregister), Arbejdsmarkedets Feriefond og Feriekonto
* Danmarks Statistik
* NemKonto
* [Pensionskasser, banker og forsikringsselskaber]
* [Foreninger]
* [Tillidsrepræsentanter og faglige organisationer]
* Arbejdsskadestyrelsen (anmeldelser om arbejdsskader)
* Arbejdsgivernes Uddannelsesbidrag (AUB)
* Arbejdsmarkedsstyrelsen (jobskabelsesordninger)
* Kommuner vedrørende dagpengerefusion
* Virk.dk
* Indkomstregistret
* DA-Barsel [og/eller Barsel.dk]
* [Virksomhedens] eksterne revision
* [Virksomhedens] eksterne rådgiver, herunder advokat/Dansk Erhverv

I tilfælde af videregivelse vil det ske inden for rammerne af databeskyttelsesreglerne.

Vi kan også vælge at bruge eksterne databehandlere f.eks. et lønbureau. I så fald indgår vi en skriftlig databehandleraftale, der sikrer, at gældende regler bliver overholdt.

**Særligt om overførsel til modtagere udenfor EU [Kun hvis relevant]**

*[Virksomhedens navn] overfører dine personoplysninger til modtagere uden for EU og EØS.*

*Det drejer sig om [indsæt modtagere i tredjelande], som er beliggende i [indsæt tredjelande].*

*Vi kan oplyse, at [indsæt oplysninger om, hvorvidt Kommissionen har truffet afgørelse om tilstrækkeligheden af beskyttelsesniveauet eller i tilfælde af overførsler i henhold til databeskyttelsesforordningens artikel 46, 47 eller 49, stk. 1, andet afsnit, en henvisning til de fornødne eller passende garantier, og hvordan den registrerede kan opnå kopi heraf, eller hvor garantierne er blevet gjort tilgængelige].*

**Sletning**

[Hvis muligt, angives tidspunkt for sletning af oplysningerne:]

Vi sletter dine personoplysninger [5 år] efter ansættelsesforholdets ophør hos [Virksomhedens navn].

Virksomheden opbevarer endvidere oplysninger omfattet af bogføringsloven i overensstemmelse med reglerne i denne lovgivning.

Hvis der er en saglig grund til at opbevare oplysninger i længere tid, kan dette ske.

**Sikkerhed**

[Virksomheden] har som dataansvarlig pligt til at beskytte de persondata, vi har om vores medarbejdere. Du kan læse mere herom i vores Sikkerhedspolitik ved personaleadministration.

**Kontaktoplysninger**

[På virksomheden uanset om databeskyttelsesrådgiver]

[Hvis virksomheden har udpeget en databeskyttelsesrådgiver, bør kontaktoplysningerne på denne fremgå her].

Hvis du har spørgsmål om [Virksomhedens navn] behandling af oplysninger om dig, er du velkommen til at kontakte [kontaktperson, f.eks. HR-afdelingen].

**Bilag 2. Eksempler på tekst om instruktion om behandling af personoplysninger samt sikkerhedsbrud**

**Din håndtering af personoplysninger og håndtering af eventuelle sikkerhedsbrud**

Som medarbejder er du forpligtet til at følge [Virksomhedens] anvisninger i forhold til behandling af personoplysninger, som måtte komme i din besiddelse som led i udførelsen af dit arbejde, og du skal reagere ved evt. sikkerhedsbrud.

**Overholdelse af instruktioner om behandling af personoplysninger**

[Virksomhedens navn] som dataansvarlig og/eller databehandler har pligt til at beskytte kunders og andre personers personoplysninger, der er i vores besiddelse.

Du er forpligtet til at overholde de til enhver tid gældende instruktioner om, hvorledes persondata skal håndteres. Instruktionerne er nærmere beskrevet [nævn folder eller skriv evt. instruktionerne her.].

**Brud på persondatasikkerheden**

Ved et eventuelt brud på persondatasikkerheden har virksomheden i nogle tilfælde en forpligtelse til at anmelde hændelsen til Datatilsynet inden for 72 timer samt at underrette de berørte personer.

I alle tilfælde af brud på persondatasikkerheden har virksomheden en forpligtelse til at dokumentere de faktiske omstændigheder ved sikkerhedsbruddet, dets virkninger og de afhjælpende foranstaltninger, som vi har truffet. Alt sammen for at kunne vise over for Datatilsynet, at vihar taget hånd om sikkerhedsbruddet.

Hvis der opstår brud på persondatasikkerheden i forbindelse med personoplysninger, som [Virksomheden] behandler for andre virksomheder/samarbejdspartnere, har vi en pligt til at underrette disse virksomheder/samarbejdspartnere.

Derfor har du som medarbejder pligt til **straks** at henvende dig til [databeskyttelsesrådgiver, persondataansvarlige [fx IT-chef, økonomichef, HR-chef osv.] og din nærmeste leder] [indsæt nærmere kontaktoplysninger], hvis du bliver opmærksom på et brud på persondatasikkerheden.

Brud på persondatasikkerheden kan f.eks. rent teknisk ske, hvis [Virksomhedens] it-systemer med personoplysninger ikke er tilstrækkelig sikret, således at udefrakommende får adgang til oplysningerne (fx hacking). Det kan imidlertid også være [Virksomhedens] egen håndtering af personoplysningerne, der kan forårsage et sikkerhedsbrud, f.eks. hvis [Virksomheden] ubeføjet videregiver eller ændrer personoplysningerne. Som eksempler på brud på persondatasikkerheden kan nævnes følgende situationer (ikke udtømmende):

* Andre personer end den eller de personer hos [Virksomheden], der er autoriseret til det, får (uautoriseret) adgang til personoplysninger. Det kan både være personer uden for eller inden for [Virksomheden].
* [Virksomhedens] medarbejdere ændrer eller sletter personoplysninger ved et uheld, eller oplysningerne går til grunde ved fx brand eller oversvømmelse.
* Brud på [Virksomhedens] server, hvor uvedkommende har fået indsigt i personoplysninger – fx kundedatabasens CPR-oplysninger, kreditkortoplysninger eller lignende.
* [Virksomhedens] medarbejdere videregiver personoplysninger – bevidst eller ubevidst – om en borger/kunde til en anden borger/kunde – eller måske ligefrem flere andre uvedkommende personer.
* Når manglende/mangelfuld kryptering af [Virksomhedens] hjemmeside indeholdende fx et kundelogin resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

Er du i tvivl om, hvorvidt der er tale om brud på persondatasikkerheden i en given situation, er det bedre at henvende dig én gang for meget end én gang for lidt.

1. [1] Se Datatilsynets ”Vejledning om fortegnelse” fra august 2020, s. 10. [↑](#footnote-ref-2)